Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

ON KUMMER'S MEMOIR OF 1857 CONCERNING FERMAT'S LAST THEOREM

By H. S. Vandiver

Department of Mathematics, Cornell University

Communicated by L. E. Dickson, March 6, 1920

The article referred to in the title appeared in the *Mathematische Abhandlungen* of the Berlin Academy for the year 1857, pp. 41–74. In the present note it will be pointed out that the proofs of the results given by Kummer are inaccurate and incomplete in several respects. The discussion will be confined exclusively to the indication of those parts of the argument which are deficient or incorrect, and in no case will methods for correcting the proofs or supplying the missing analysis be considered here.

In the first place Kummer divides his work, as usual, into the discussion of the two cases arising from

$$x^\lambda + y^\lambda + z^\lambda = 0 \tag{1}$$

where x, y and z are rational integers and λ is an odd prime. The *first case* arises in the consideration of (1) when xyz is prime to λ, and the *second case* when xyz is divisible by λ.

For the first case he shows that if (1) is satisfied then $B_{(\lambda-3)/2}$ and $B_{(\lambda-5)/2}$ are each divisible by λ, the B's being Bernoullian numbers,

$$B_1 = {}^1/_6,\ B_2 = {}^1/_{30},\ \text{etc.}$$

The proof is given on pages 61–65 of the article in question. No criticisms will be made here of this part of the work.

For the second case Kummer concludes that the relation (1) is impossible under the three assumptions:

1. *The first factor of the class number H is divisible by λ but not by λ^2*

2. *If* $B_\nu \equiv 0 (\text{mod } \lambda)$, $\nu < {}^1/_2(\lambda - 1)_2$, *there exists an ideal in the field* $\Omega(\alpha)$, $\alpha^\lambda = 1$, $\alpha \pm 1$, *with respect to which as a modulus the unit*

$$E_\nu(\alpha) = \prod_{k=0}^{\mu-1} e(\alpha^{\gamma^k})^{\gamma^{-2k\nu}}$$

is not congruent to the λth power of an integer in $\Omega(\alpha)$.

3. *The Bernoullian number $B_{\nu\lambda}$ is not divisible by λ^3.*

In the above assumptions $H = h_1, h_2$, where

$$h_1 = \frac{P}{(2\lambda)^{\mu-1}},\ h_2 = \frac{D}{\Delta},\ \mu = \frac{\lambda-1}{2},$$

and P, D and Δ are defined as follows:

Let β be a primitive root of $\beta^{\lambda-1} = 1$ and λ a primitive root of λ. Then

$$P = \prod_{j=1}^{\mu} \phi(\beta^{2j-1}),\ \phi(\beta) = 1 + \gamma_1\beta + \gamma_2\beta^2 + \ldots\ldots + \gamma_{\lambda-2}\beta^{\lambda-2}$$

where γ_i is the least positive residue of γ^i modulo λ Also

$$e(\alpha) = \sqrt{\frac{(1-\alpha^\gamma)(1-\alpha^{-\gamma})}{(1-\alpha)(1-\alpha^{-1})}},$$

and if lx denotes the real value of log x, then

$$D = \begin{vmatrix} le(\alpha), & le(\alpha^{\gamma}) \ldots\ldots\ldots & le(\alpha^{\gamma^{\mu-2}}) \\ le(\alpha^{\gamma}), & le(\alpha^{\gamma^2}) \ldots\ldots\ldots & le(\alpha^{\gamma^{\mu-1}}) \\ & \ldots\ldots\ldots\ldots & \\ & \ldots\ldots\ldots\ldots & \\ le(\alpha^{\gamma^{\mu-2}}), & le(\alpha^{\gamma^{\mu-1}}) \ldots\ldots & le(\alpha^{\gamma^{2\mu-4}}) \end{vmatrix}.$$

If $\epsilon_1(\alpha)$, $\epsilon_2(\alpha), \ldots\ldots \epsilon_{\mu-1}(\alpha)$ are fundamental units in $\Omega(\alpha)$, that is, units which have the property that all units in the field can be expressed as products of powers of them multiplied by $\pm\alpha^m$, then

$$\Delta = \begin{vmatrix} l\epsilon_1(\alpha) \ldots\ldots\ldots\ldots & l\epsilon_{\mu-1}(\alpha) \\ \ldots\ldots\ldots\ldots & \\ \ldots\ldots\ldots\ldots & \\ l\epsilon_1(\alpha^{\gamma^{\mu-2}}) \ldots\ldots & l\epsilon_{\mu-1}(\alpha\gamma_{\mu-2}) \end{vmatrix}.$$

To establish the above result Kummer essays to prove four direct theorems in the theory of the field $\Omega(\alpha)$. These theorems are set forth later in this note and numbered I to IV. As will be shown, the proofs of theorems I and IV are incomplete as several unproved statements are made and the proofs of II and III are inaccurate, since use is made of a formula which is not true in general.

In *Crelle*, **44,** 1852 (134), Kummer gave the relation

$$(\lambda - 1)l\left(\frac{(\varphi(\alpha)}{\varphi(1)}\right) \equiv l\left(\frac{N\varphi(\alpha)}{[\varphi(1)]^{\lambda-1}}\right) + \sum_{i=0}^{\lambda-2} \frac{d_o{}^{i\lambda^n} l\varphi(e^v)}{dv^{i\lambda^n}} X_i(\alpha) \qquad (2)$$

modulo λ^{n+1}. In this formula $\varphi(\alpha)$ is an algebraic integer in the field $\Omega(\alpha)$, and the symbol

$$l\left(\frac{\varphi(\alpha)}{\varphi(1)}\right)$$

modulo λ^{n+1}, represents that part of the logarithmic series

$$\frac{\varphi(\alpha) - \varphi(1)}{\varphi(1)} - \frac{1}{2}\left(\frac{\varphi(\alpha) - \varphi(1)}{\varphi(1)}\right)^2 + \frac{1}{3}\left(\frac{(\varphi(\alpha) - \varphi(1)}{\varphi(1)}\right)^3 \ldots\ldots\ldots$$

none of whose terms are divisible by λ^{n+1}. The symbol $N\varphi(\alpha)$ stands for the norm of $\varphi(\alpha)$ and

$$\frac{d_o{}^s l\varphi(e^v)}{dv^s}$$

indicates that log $\varphi(e^v)$ is to be differentiated s times and zero substituted for v in the result. Further,

$$X_i(\alpha) = \alpha + \gamma^{-i\lambda^n}\alpha^{\lambda} + \gamma^{2i\lambda^n}\alpha^{\gamma^2} + \ldots\ldots + \gamma^{-(\lambda-2)i\lambda^n}\alpha^{\gamma^{\lambda-2}}.$$

F. Mertens (*Wiener Berichte*, **126,** 1917, Abt. II*a*, pp. 1337–43) points out that the relation (2) is not true in all cases and shows that an error occurs in Kummer's argument on page 133 of the latter's paper.

We shall now examine Kummer's 1857 memoir in detail and in the light of what has just been mentioned.

Under assumption 1, given above, namely, that h_1 is isdivible by λ but not by λ^2, Kummer proceeds to show that only one of the numbers B_i, $i = 1, 2, \ldots\ldots, \mu - 1$, is divisible by λ. In this connection he states (p. 42, 5th line from bottom) "....denn der erste Faktor der Klassenanzahl muss, wie aus meiner Untersuchung der Teilbarkeit der Klassenanzahl durch λ (*Liouville's Journal*, **16**, 1851 (473)) unmittelbar folgt, den Faktor λ mindestens so viel mal enthalten, als wie viele der $(\lambda - 3)/_2$ Bernoullischen Zahlen durch λ theilbar sind." On examining the paper referred to by Kummer we find that he reduces h_1 modulo λ and obtains a residue which may be expressed in the form

$$m\prod_{i=1}^{\mu-1} B_1$$

where m is an integer prime to λ. At no place in this work however, does he refer to any reduction of h_1, modulo λ^n, $n > 1$. Hence, he is not warranted in making, without additional argument, the statement given above.

Having concluded that only one of the first $\mu - 1$ Bernoullian numbers is divisible by λ, Kummer calls this one B_ν and derives (p. 44), under assumption 1, the following:

Theorem I. *If* $B_\nu \equiv 0 \pmod{\lambda}$, *and* $h_2 \equiv 0 \pmod{\lambda}$ *then* $E_\nu(\alpha)$ *is the* λ^n *power of a unit in* $\Omega(\alpha)$.

On page 45 an attempt is made to prove, under assumption 1, the

Theorem II. *If* $B_\nu \equiv 0 \pmod{\lambda}$ *but* $B_{\nu\lambda} \equiv 0 \pmod{\lambda^3}$ *then a unit in* $\Omega(\alpha)$ *which is congruent modulo* λ^2 *to a rational integer is the* λ_{th} *power of a unit in* $\Omega(\alpha)$.

In the argument covering this (p. 46), there is used the incorrect formula (2) of this paper. Also, on page 50, under assumption I, is given the

Theorem III. *If* $F(\alpha)$ *is an integer in the field* $\Omega(\alpha + \alpha^{-1})$ *and if*

$$\frac{d_o^{2\nu} lF(e^\nu)}{dv^{2\nu}} \equiv 0 \pmod{\lambda}$$

then a unit $E(\alpha)$ *in* $\Omega(\alpha)$ *can be found such that*

$$E(\alpha)F(\alpha) \equiv a \pmod{\lambda}$$

where a is a rational integer.

In proving the above, the incorrect relation (2) is again used.

In paragraphs 4, 5 and 6, pp. 50–61, Kummer goes through a course of reasoning which leads him to

Theorem IV. *If* P *is an ideal such that* P^λ *is the principal ideal* $(F(\alpha))$, *and* $B_\nu \equiv 0$ (mod. λ) *then* P *is or is not a principal ideal according as*

$$\frac{d_o^{\lambda - 2\nu} lF(e^v)}{dv^{\lambda - 2\nu}} \equiv \text{ or } 0 \substack{+\\ \ddagger \\ +} \pmod{\lambda}.$$

In this connection note the formula (A) which he gives on page 53. The number $\Psi_r(\alpha)$ which appears here is defined as the product of certain ideal factors (11th line from bottom); but this decomposition holds for the case where $\Psi_r(\alpha)$ contains only ideals of the first degree. Kummer has himself given (*Crelle*, **44**, p. 120) the decomposition for the generalized function $\Psi_r(\alpha)$ which may contain ideals of other degrees than the first and said decomposition is of a more general form than that which applies for ideals of the first degree. It would follow from these facts that in theorem IV, $F(\alpha)$ would necessarily contain factors of the first degree only. However, on page 67 of the 1857 memoir the theorem is applied to certain ideals $\Theta_r(\alpha)$ which are not proved to be of the first degree.

Also, on page 54 it is stated without proof or reference that if m is not divisible by λ-1 then

$$\frac{d_o^{m\lambda^r} l\phi(e^v)}{dv^{m\lambda^r}} \equiv \frac{d_o^{m\lambda^r} l\phi_1(e^v)}{dv^{m\lambda^r}} \pmod{\lambda^{r+1}}$$

where $\phi(\alpha)$ and $\phi_1(\alpha)$ are integers in $\Omega(\alpha)$ such that $\phi(\alpha) \equiv \phi_1(\alpha) \pmod{\lambda^{r+1}}$. The writer has not been able to find a proof of this any where in Kummer's papers.

AN IMPROVED FORM OF HIGH TENSION D. C. APPARATUS

BY DAVID L. WEBSTER

DEPARTMENT OF PHYSICS, MASSACHUSETTS INSTITUTE OF TECHNOLOGY

Communicated by E. B. Wilson, March 6, 1920

In a recent paper on X-rays in these PROCEEDINGS,[1] I described a high tension D. C. outfit based on that of A. W. Hull, with certain changes of details. On further investigation it has appeared that one of these changes introduces a disturbing factor, which was not large enough to affect the results in that paper, or to be detected by the tests for fluctuation used at that time, but which might have been detectable if the choke coils in the apparatus had not had extremely high inductances. As I have received several inquiries lately about the best way to build such an outfit and the question is of importance to X-ray research workers, I am writing this note to call attention to the existence of this disturbing factor and the way to eliminate it in outfits with inductances and capacities not so large as those used here.

In the arrangement described in the previous paper the principal A. C. components on the D. C. line had a frequency of 1000 cycles per second, twice that of the primary current, and the currents in both sides of the line increased and decreased in the same phase. The disturbing factor was the capacity of the transformer secondary, relative to the ground, that introduced components of current at 500 cycles, with opposite phases on the two sides of the line. Because of this phase relation, the 500 cycle components are difficult to choke off unless the middle points of the D. C. condenser lines are grounded, in which case the phase relation of each type